IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Levy
Application No: 10/797,920
Filed: March 9, 2004
For: METHOD AND APPARATUS FOR CONTENT IDENTIFICATION/CONTROL
Examiner: Stanley, Mark P.
Date: October 21, 2009

Art Unit: 2623
Confirmation No.: 3347
VIA ELECTRONIC FILING

APPEAL BRIEF

Mail Stop: Appeal Brief – Patents
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is responsive to the *Notice of Appeal* filed August 21, 2009, and the *Notice of Panel Decision from Pre-Appeal Brief Review* mailed September 11, 2009.

The Office is authorized to charge our Deposit Account No 50-1071 for any fees that may be required in connection with filing of this Appeal Brief.

I. REAL PARTY IN INTEREST

The real party in interest is Digimarc Corporation of Beaverton, Oregon.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

Claims 1, 4, 7-11, 13-18, and 25-31 are finally rejected and appealed.

Claims 2-3, 5-6, 12 and 19-24 are canceled.

IV. STATUS OF AMENDMENTS

All prior amendments have been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed technology relates to protecting content (*e.g.*, video) against unauthorized redistribution from an intended destination, while still allowing a consumer some flexibility in sharing the content among various computers, iPods, etc.

One aspect of the claimed technology (independent claim 11) involves content formatted in an IP packet that includes a destination address in the header.[1] The address

[1] Specification, *e.g.*, at page 5, line 3.

corresponds to a device at a first location where delivery of the packet was intended by an originator thereof.[2] This much is conventional.

In accordance with claim 11, when the packet is at the first physical location, additional data in the packet header is interpreted as specifying whether it is permissible to re-transmit a copy of content data in the packet (after receipt at the first destination address) to a second destination address.[3]

In particular, if this additional header data has a first state, then re-transmission of the content data is prohibited to any second destination address.[4]

However, if this additional header data has a second state, then re-transmission of the content data is prohibited to any second address other than a second destination address within a domain that also includes the first destination address.[5]

Consider college students A and B – each with a computer in a common domain (*e.g.*, an Ethernet network of a dormitory). Student A's computer receives content in packet form, addressed to it by a content originator (*e.g.*, a movie service). If additional data in the packet header has the second state, student A's computer can re-transmit this content to student B's computer – since they are both in the same domain (i.e., the domain to which delivery of the packet was intended by the originator). However, student A cannot re-distribute this content to student C at a different university.

Unlike the cited art, the decision of whether to permit re-distribution of the content packet to a *second* destination address is a function of the *first* destination address.

Another aspect of the claimed technology (independent claim 4) is similar, but more particularly focuses on the home network scenario, i.e., governing potential redistribution of content from the home.[6]

[2] *Ibid*, page 8, lines 5-6.

[3] Specification, *e.g.*, page 9, lines 1-3; Fig. 3 at box 330.

[4] Specification, *e.g.*, at page 10, lines 1-4; page 14, lines 3-15.

[5] *Ibid*.

[6] Specification, *e.g.*, at page 5, lines 2-3.

In accordance with claim 4, a distributor provides entertainment content in IP packet form to a first destination address within the home, to which the distributor intends the content to be delivered.[7]

The distributor forms the header data with additional data specifying whether it is permissible to send a copy of the content data to a second, different, destination address.[8]

Again, this additional header data has two states. If the additional header data has a first state, then it is not permissible to send a copy of the content data to any second destination address.[9]

However, if the additional header data has a second state, then it is not permissible to send the content to any second destination address except to a second destination address within a domain that also includes the first destination address. [10] The claimed domain "comprises networked devices associated with a single family."[11]

If a husband and wife each have a computer coupled to a wireless home network, and the husband purchases a movie delivered to his computer, which arrives with additional header data that is in the second state, then he can re-distribute the content to the wife's computer. But he cannot redistribute the content to his office computer (since it is not in the home domain – the destination to which the movie service sent the movie).

Again, unlike the cited art, the decision of whether to permit re-distribution of the content packet to a *second* destination address is a function of the *first* destination address.

[7] Specification, *e.g.*, at page 5, lines 5-8.

[8] Specification, *e.g.*, page 9, lines 1-3; Fig. 3 at box 330.

[9] Specification, *e.g.*, at page 10, lines 1-4; page 14, lines 3-15.

[10] *Ibid.*

[11] Specification, *e.g.*, at page 4, line 31.

Independent claim 25 concerns a somewhat different aspect of Appellant's technology. Again, the claim concerns deterring unauthorized redistribution of content (video entertainment) from a consumer's home network.[12] The network includes at least a computing device[13] and a networking device.[14]

In accordance with claim 25, the computing device ascertains restriction information for the video entertainment.[15] (This is done by extracting the restriction information from header data.[16] Or by obtaining the restriction information from a remote repository associated with the video entertainment.[17] Or by discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment.[18])

After it has ascertained the restriction information for the video, the computing device in the home network divides the video entertainment among plural IP packets,[19] and includes data indicating the ascertained restriction information in the header of each packet.[20] The computing device in the home network then sends these packets to the home network's networking device.[21]

The home network's networking device then examines the just-included data in the packets. [22] The home networking device refuses to transmit the packets to a different network if this included data indicates that the video should not be redistributed from the consumer's home network.[23]

[12] Specification, *e.g.*, at page 5, lines 2-8.
[13] Specification, *e.g.*, at page 10, lines 24-25.
[14] Specification, *e.g.*, at page 5, line 21, page 11, lines 24-30.
[15] Specification, *e.g.*, at page 10, lines 30-31.
[16] *Ibid.*; Fig. 1, block 200.
[17] Specification, *e.g.*, at page 7, lines 8-9; page 9, lines 5-6; page 10, lines 10-11 and 27.
[18] Specification, *e.g.*, at page 11, lines 14-16.
[19] Specification, *e.g.*, at page 7, lines 13-20, page 10, lines 24-25.
[20] Specification, *e.g.*, at page 7, lines 16-20, page 11, lines 3-4.
[21] Specification, *e.g.*, at page 7, lines 17-23.
[22] Specification, *e.g.*, at page 14, lines 6-9.
[23] Specification, *e.g.*, at page 7, lines 22-23; page 14, lines 6-9.

Independent claim 1 also concerns enforcing restrictions on redistribution of content in packet form.

In accordance with claim 1, a geographical boundary across which certain content does not pass is defined – at least in part – by a hardware firewall device.[24] (Most network routers commonly include hardware firewalls.[25])

The method determines whether an IP packet conveys content that should not cross this boundary, by reference to one or more single-bit flags included in header data of the packet.[26]

The claim further specifies that the one or more of the flag bits is related to the payload of a watermark in the content data.[27]

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 11, 14 and 15 are rejected as non-statutory under §101.

Claims 4, 7-9, 11 and 13-17 are rejected as anticipated by Roese (20030217122).

Claims 1, 10, 18, 25-26 and 28 are rejected as obvious over Roese in view of Levy '899 (20010044899).

Claim 27 is rejected over Roese in view of Levy '899, and further in view of Levy '844 (20020186844).

Claim 29 is rejected over Roese in view of Levy '899 and further in view of Medvinsky (20050071663).

Claims 30-31 are rejected over Roese in view of Medvinsky.

[24] Specification, *e.g.*, at page 3, lines 5-10; page 6, lines 23-27; Fig. 1, block 110.

[25] Specification, *e.g.*, at page 11, lines 26-30.

[26] Specification, *e.g.*, at page 3, lines 7-8; page 10, lines 2-4; page 14, lines 6-9.

VII. ARGUMENT

1. Rejection of claims 11, 14 and 15 under §101

The state of the law with respect to subject matter eligibility is in flux; the Supreme Court may clarify applicable standards in the pending *Bilski* case.[28] However, even under the interpretation currently applied by the Office, claims 11, 14 and 15 concern patentable subject matter.

For example, although claim 11 is drawn to a method of data processing, the data represents physical things, and the method is tied to a machine.

Claim 11 recites "…the first destination address corresponding to a device at a first physical location." The "device" is, *e.g.*, a computer, set-top box or the like to which the packet data is addressed. The claim states that it has a "physical" location. The claim does not simply claim an abstract idea, a mental process, or substantially all practical uses of a law of nature or a natural phenomenon.

Moreover, the cited language ties the method to a machine, i.e., the "device at a first physical location" to which the first destination address corresponds.

Similarly, claim 11 specifies "*…the body data comprising content data…*" Construed with reference to the specification, "content" refers to audio, video, etc.[29] Such content represents physical things, *e.g.*, sound pressure waves in the case of audio, and objects and scenes depicted in the video.

Dependent claim 14 further emphasizes physicality. The claim notes that a "device" (a physical object) associated with the second destination address has a second physical location. The claim continues to define the invention in terms of relationships

[27] Specification, *e.g.*, at page 7, lines 3-7 and 20-22; page 11, lines 12-16, Fig. 1, blocks 210 and 220.

[28] Hirshfield, Interim Examination Instructions For Evaluating Subject Matter Eligibility Under 35 U.S.C. § 101, USPTO Memo To TC Directors, August 24, 2009.

[29] Specification, *e.g.*, at page 1, lines 4-5, "*The present invention relates to identification and control of electronic content (e.g., audio, video, etc.)*" *See, also*, reference to a video of a New York Yankees baseball game as

between physical locations (*e.g.*, "*if the second physical location is physically proximate to the first physical location, permitting copying of data…*").

Accordingly, claim 11, and dependent claims 14 and 15, are statutory under Section 101.

2. Claim 4 (§102 Roese)

Claim 4 reads as follows:

> *4. A method of providing entertainment content from a distributor to a home, while governing potential redistribution of the content from the home, the method including forming an IP packet having header data and body data, wherein the body data includes content data, and the header data includes a first destination address within the home to which the distributor intends the content data be delivered, the method comprising:*
>
> *the distributor forming said header data to additionally include additional data specifying whether it is permissible to send a copy of the content data in the packet to a second destination address different than the first destination address, wherein the additional data has at least two states, respectively indicating:*
>
> *(a) it is not permissible to send a copy of the content data in the packet to any second destination address; or*
>
> *(b) it is not permissible to send a copy of the content data in the packet to any second destination address except to a second destination address within a domain that also includes the first destination address; and*
>
> *wherein said domain comprises networked devices associated with a single family, and restriction on potential redistribution of the content is defined by reference to the intended first address.*

As discussed above, claim 4 is drawn to a method of providing entertainment content from a distributor to a home. For example, a pay per view sports network may deliver a baseball game to a consumer.

The content data is transmitted in packets that identify the intended destination – within a home (i.e., the first destination address). The distributor intends the content to be received by the first destination address.

illustrative content, page 2, lines 4-10.

The claimed arrangement concerns potential re-distribution of the content, *e.g.*, the consumer having a device that forwards received packets from the intended recipient address (within the home) to another address (*e.g.*, a friend's house).

To address such potential re-distribution, the claimed method specifies that the distributor forms the header data so as to include "additional data" specifying whether it is permissible to send a copy of data in the packet to a second destination address.

This "additional data" has one of two states. State 1 indicates it is not permissible to send a copy of the content data anywhere else (i.e., it is forbidden to send the content data to any second destination address).

State 2 is more permissive. State 2 indicates it is not permissible to send a copy of the content data anywhere else *except to an address within a domain that also includes the first destination address* (i.e., in the home). Such limited redistribution is permitted.

Roese does not teach each of the claim's limitations.

As shown in Roese's Fig. 6, and paragraphs [0115] – [0117], his arrangement inserts a tag in certain packets. This tag indicates that the packets should not be accessed if found outside a specified location (*e.g.*, outside a particular campus, etc.). His tag thus has only a single state. His tag only indicates a single type of restriction:

> [0116] If system 100 determines (step 610) that the data is location sensitive, system 100 tags (step 620) the data. For example, the application generating the data and/or the server generating a data packet to transport the data over the network can add this tag while generating the data and/or packet. In one example, the tag comprises a file header that identifies location restrictions.

In *Response to Arguments* included with the Final Rejection, the Office contends:[30]

> Applicant does not clearly define the role of the distributor in the claim limitations, mainly Applicant does not differentiate whether the distributor may or may

[30] Final Rejection, page 2, lines 5 *et seq.*

> not be the same entity as that of the first destination address and whether the user may be the distributor and the user provision the entertainment content to a first destination address such as a home personal computer via actual use of the home personal computer…

The meaning of the Office's statement is unclear. However, the claim language is clear. As the claim states, the method is drawn to "*providing entertainment content <u>from a distributor to a home</u>, while governing potential redistribution of the content from the home….*"

An interpretation of the claim that somehow makes the user in the home also the claimed "distributor" is too tortured to be sustained.

(Would a home user form packet header data with the "additional data" having the two specified states, as required by the "distributor" in the claim?)

In the present arrangement, re-distribution <u>is conditioned on a relation between two addresses</u>: the re-distribution address and the initial address (assuming the flag is in the second state). That is, if the re-distribution address is in the same (home) domain as the first address, redistribution is permitted. Else, not.

Roese lacks these concepts

Instead, Roese makes all delivery decisions (initial distribution and re-distribution) based on location. Roese does not test any relation between an original address and a subsequent address in deciding whether re-distribution is permitted.

In some cases, Roese's *result* may be the same as Appellant's *result* (re-distribution might be denied), but the *method* of reaching the result is different. At issue is the *method* – not the result. (A claim may concern a method of losing weight – by liposuction. Prior art may teach a different method of losing weight – by exercise and restricting caloric intake. The latter doesn't anticipate the former, even though the result may be the same.)

The Final Rejection is grounded, improperly, on the sometimes-similarity of *result.*

Roese does not teach:

> *the distributor forming header data to additionally include additional data specifying whether it is permissible to send a copy of the content data in the packet to a second destination address different than the first destination address, wherein the additional data has at least two states, respectively indicating:*
>
> *(a) it is not permissible to send a copy of the content data in the packet to <u>any</u> second destination address; <u>or</u>*
>
> *(b) it is not possible to send a copy of the content data in the packet to any second destination address <u>except to a second destination address within a domain that also includes the first destination address</u>.*

Moreover, claim 4 specifies that the domain comprises networked devices "*associated with a single family.*" Again, Roese has no such teaching.[31]

Finally, claim 4 explains "*restriction on potential redistribution of the content is defined <u>by reference to the intended first address</u>.*" The restriction in Roese is not defined by reference to the intended first address.

Because Roese does not teach each limitation of the claimed method, the anticipation rejection should be reversed.

3. <u>Claim 7 (§102 Roese)</u>

Claim 7 is allowable for its dependence from claim 4, and is also independently patentable. The claim reads as follows:

[31] The Office mapped the "single family" limitation to "network devices within a campus." See Final rejection, page 5, last sentence.

> *7. The method of claim 4 wherein a device associated with the first destination address has a first physical location and a device associated with the second destination address has a second physical location, and the additional data includes a field signaling that copying of data in said packet to said second destination address should be:*
>
> *(a) permitted if the second physical location is physically proximate to the first physical location; and*
>
> *(b) prohibited if the second physical location is physically remote from the first physical location.*

The Final rejection cites Roese at paragraphs [0100] – [0103] for such limitations. However, those paragraphs concern restricting network log-ins based on a user's GPS- or other location-authenticated information. They do not concern re-distribution of entertainment content from an intended destination address to a second address.

Again, Roese fails to teach the claim limitations. The anticipation rejection should be reversed.

4. <u>Claim 8 (§102 Roese)</u>

Claim 8 is allowable for its dependence from claim 7, and is also independently patentable. The claim reads as follows:

> *8. The method of claim 7 wherein the first and second destination addresses are within a common domain.*

The Final Rejection cited the same paragraphs from Roese ([0100] – [0103]) relating to GPS-authenticated log-ins to secure networks. They do not teach the claimed arrangement.

The Final Rejection also cites Roese Figs. 1 and 8, noting that the first and second destination devices <u>*can be*</u> within a common domain. The figures show:

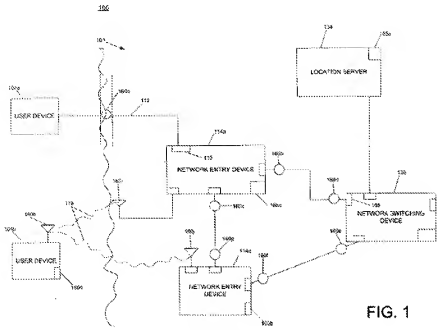

FIG. 1

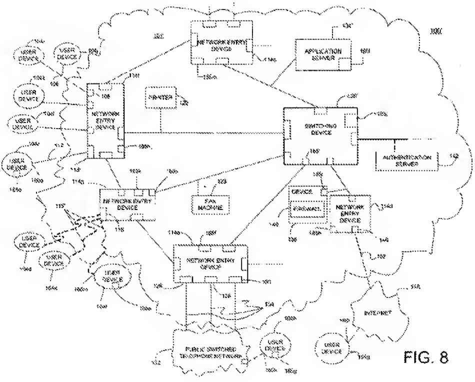

FIG. 8

Roese's Figs. 1 and 8 have no teachings about a common domain. What "*can be*" is not the test of anticipation.

Again, the anticipation rejection should be reversed.

5. <u>Claim 9 (§102 Roese)</u>

Claim 9 is allowable for its dependence from claim 7, and is also independently patentable. The claim reads as follows:

> *9. The method of claim 7 wherein the first and second destination addresses both correspond to network devices associated with a single family.*

The Office contends that the "network devices associated with a single family" is anticipated because Figs. 1 and 8 of Roese <u>may be</u> limited to a single family.

Again, what "may be" is not the test of anticipation. What "is" is.

Because Roese does not teach the arrangement of claim 9, the rejection should be reversed.

6. <u>Claim 11 (§102 Roese)</u>

Claim 11 reads as follows:

> *11. A method of data processing that includes receiving an IP packet having header data and body data, wherein the header data includes a first destination address, the first destination address corresponding to a device at a first physical location where delivery of the packet was intended by an originator thereof, the body data comprising content data, the method comprising – at said first physical location - interpreting additional data in the header of said packet as specifying whether it is permissible to re-transmit a copy of data in the packet - after receipt thereof at the first destination address - to a second destination address, wherein:*
>
> *(a) if the additional data has a first state, prohibiting re-transmission of a copy of the content data in the packet to any second destination address; and*
>
> *(b) if the additional data has a second state, prohibiting re-transmission of a copy of data in the packet to any second destination address other than a second destination address within a domain that also includes the first destination address.*

Claim 11 is similar to claim 4, but is lacking certain of its limitations. Nonetheless, it is not anticipated by Roese.

Again, Roese does not include additional data in his packet that can have two states, respectively indicating the two claimed restrictions on re-transmission.

Again, Roese does not teach an arrangement in which a decision whether to re-transmit a content packet to a *second* destination address ("after receipt thereof at the first destination address") is a function of the *first* destination address, as claimed.

Again, claim 11 is not anticipated by Roese.

7. Claim 13 (§102 Roese)

Claim 13 is allowable for its dependence from claim 11, and is also independently patentable. The claim reads as follows:

> *13. The method of claim 11, wherein said domain comprises networked devices associated with a single family.*

The Office rejects this claim by reference to its rejection of independent claim 4. In that rejection, the Office mapped the "single family" limitation to "network devices within a campus."[32] A campus is not a "single family," as claimed.

Again, the rejection should be reversed.

8. Claim 14 (§102 Roese)

Claim 14 is allowable for its dependence from claim 11, and is also independently patentable. The claim reads as follows:

[32] Final rejection, page 5, last sentence.

> *14. The method of claim 11 wherein a device associated with the second destination address has a second physical location and wherein:*
> *(a) if the second physical location is physically proximate to the first physical location, permitting copying of data in said packet to the second destination address; and*
> *(b) if the second physical location is physically remote from the first physical location, prohibiting copying of data in said packet to the second destination address.*

The Office rejects this claim by reference to its rejection of dependent claim 7.

As noted above, cited Roese paragraphs [0100] – [0103] concern restricting network log-ins based on a user's GPS- or other location-authenticated information. They do not concern re-distribution of entertainment content from an intended destination address to a second address, as claimed.

Again, Roese does not anticipate the method of claim 14.

9. <u>Claim 15 (§102 Roese)</u>

Claim 15 is allowable for its dependence from claim 14, and is also independently patentable. The claim reads as follows:

> *15. The method of claim 14 wherein the first and second destination addresses are within a common domain.*

The Office rejects this claim by reference to its rejection of dependent claim 8.

As noted above, Roese's cited Figs. 1 and 8 have no teachings about a common domain. What "*can be*" is not the test of anticipation.

Again, the anticipation rejection should be reversed.

10. <u>Claim 16 (§102 Roese)</u>

Claim 16 is allowable for its dependence from claim 14, and is also independently patentable. The claim reads as follows:

> *16. The method of claim 14 wherein the first and second destination addresses both correspond to network devices associated with a single family.*

The Office rejects this claim by reference to its rejection of dependent claim 9, which contends that the "network devices associated with a single family" is anticipated because Figs. 1 and 8 of Roese <u>may be</u> limited to a single family.

Again, what "may be" is not the test of anticipation.

Again, the rejection of claim 16 should be reversed.

11. <u>Claim 17 (§102 Roese)</u>

Claim 17 is allowable for its dependence from claim 14, and is also independently patentable. The claim reads as follows:

> *17. The method of claim 14 wherein the method includes determining whether the second physical location is physically remote from the first physically location by reference to whether the second destination address is served by a common firewall with the first destination address.*

The Office cites Roese paragraph [0098] as teaching a firewall. It does.

However, Roese's system discussed in paragraph [0098] is "location aware,"[33] such as through use of GPS receivers in the various components.[34] Roese's firewall is a way to enforce location-based restrictions determined by the "location aware" features of his system.

Roese does not teach use of a firewall to determine *whether* devices are physically remote or not, as presently claimed. That function is performed through use of Roese's GPS components. Accordingly, the anticipation rejection of claim 17 should be reversed.

[33] Paragraph [0098], 7th line from bottom.

12. Claim 1 (§103 Roese + Levy '899)

Claim 1 reads as follows:

> *1. A method of enforcing geographical restrictions on content redistribution in a TCP/IP network in which content is distributed in packet form, each packet including header data and content data, the header data comprising information about the packet and its payload, the method comprising the acts:*
>
> *defining a geographical boundary across which certain content data does not pass, wherein said boundary is defined – at least in part – by a hardware firewall device; and*
>
> *determining whether an IP packet should be regarded as conveying content that should not cross said boundary, by reference to one or more single-bit flags included in the header data of said packet;*
>
> *wherein said one or more flag bits are related to the payload of a watermark in the content data.*

Like claim 17 just-discussed, claim 1 requires use of a firewall to "*define*" a geographical boundary. Roese uses a firewall only to *enforce* a location-based determination made by another system component (paragraph [0098]). He does not teach use of a firewall to *define* the geography of the boundary.

Roese's discussion of "*Restricting Location of Data*" begins at paragraph [0114]. He explains that data may be restricted to a device, a home, a courtroom, a campus, a city, a country, etc. (Paragraphs [0115] – [0116].)

If Roese's data is location-restricted, he *tags* it before sending it to the requested destination (top lines of paragraph [0116]). Devices in his system that encounter the data then examine the tag. If the data is found outside the permitted location, it is destroyed, or access to it is denied (top lines of paragraph [0116]).

Roese does not teach use of a firewall in connection with *defining* a geographical boundary, as claimed. Because Roese does not teach that for which it has been cited, *prima facie* obviousness has not been established.

[34] *See, e.g.*, Roese at paragraph [0055].

Moreover, claim 1 requires one or more "single bit flags" to signal whether content should not cross a geographical boundary. The Final Rejection indicates that such limitation is taught by Roese paragraphs [0115] – [0118], and his Fig. 6. But nowhere in those 75 lines of text, nor drawing, is there any teaching of single-bit flags.

(In the later rejection of claims 30-31, on page 15 of the Final Rejection, the Office admits "Roese … do not explicitly state the use of a single bit flag." The Office then relies on Medvinsky for such "single bit flag" teaching.)

Again, because Roese does not teach that for which it has been cited, *prima facie* obviousness has not been established.

The obviousness rejection of claim 1 combines Roese with the present inventor's prior digital watermarking work in Levy '899.

Digital watermarking is the science of hiding information in other data. Thus, for example, least-significant bits of pixel data can be replaced with bits representing a text message payload. The change is too subtle for humans to discern from inspection of the altered imagery, but computer analysis can recover the hidden text payload.

Levy '899 concerns the problem wherein converting the format of content can sometimes make digital watermark data in the content unrecoverable. Thus, Levy '899 teaches that – prior to format conversion, any watermark payload should be decoded from the content. Then, after format conversion, the watermark payload is re-encoded into the content using a watermark format that is suited to the content's new format. This process (termed "transmarking") assures that the watermark has robustness or perceptibility characteristics suited for the new content format. (Levy '899 at paragraph [0007].)

In paragraph [0035] Levy '899 makes its sole references to IP packets. In particular, the present inventor teaches that when content is transformed into packet form, a watermark in the original content can be decoded, and re-encoded in the individual packets. In another arrangement, he explains that the decoded watermark can be re-encoded *after* the signal is re-combined (i.e., after the packets reach their destination, and the content is re-assembled from the individual packets). In this latter arrangement, a command is inserted into the packets' headers, detailing the watermark payload that should be re-encoded in the content after combination, and the watermarking protocol that should be used.

The Final Rejection contends that Levy '899 teaches "*...said one or more flag bits are related to the payload of a watermark in the content data*," as required by the last clause of claim 1 (page 10, first full paragraph).

There are several problems with the Office's proposed combination of Roese with Levy '899.

One is that Levy '899 takes – *as a given* – that the content is watermarked. Levy's concern is how to prevent the existing watermark from being degraded by various content conversions.

Roese does not teach or suggest any watermarking.

The Office's rationale for the combination *presumes* that the content is *already* watermarked. It proposes "*transmarking* <u>*an initial*</u> *digital watermark of the content into watermark payloads in each packet...*" (Final Rejection, top of page 11).

But this presumes too much. It presumes there <u>is</u> "an initial digital watermark." Roese does not teach one. The obviousness rationale is thus grounded on a faulty premise.

The Final Rejection later suggests that an artisan might employ a watermark because it provides "restriction information hidden from a user" (page 11, line 11). But this rationale is also faulty. The information is not hidden if it is also expressed in the packet header.

The Office blurs the two different packet-related arrangements taught in paragraph [0035] of Levy '899.

In the first arrangement, a watermark payload in the original content is re-encoded into the individual packets of content data. In this arrangement, there is no involvement of the packet header: the watermark payload is conveyed by subtle alterations to the divided content data in the packet bodies. The payload is hidden, but it is not in the headers.

In the second, a watermark payload in the original content is conveyed by the packets' headers, so that it can be re-encoded into the content when the content is later re-assembled from the individual packets. In this case, the payload is not hidden.

An artisan would not employ watermarking to provide "restriction information hidden from a user" as asserted in the Final Rejection (page 11, line 11), if the restriction information is also exposed in the packet header (page 11, line 3) – as proposed by the Rejection and required by the claim. Again, *prima facie* obviousness has not been established.

The rejection fails for lack of a rational underpinning. The Action fails to address why an artisan would have provided flag bits in packet headers, related to the payload of a watermark in content data. No reason for this dualistic approach is offered.

Having failed to establish *prima facie* obviousness, the rejection of claim 1 should be reversed.

13. <u>Claims 10 and 18 (§103 Roese + Levy '899)</u>

Claim 10 is allowable for its dependence from claim 4, and claim 18 is allowable for its dependence from claim 11. The claims are also independently patentable. The claims read as follows:

> *10[18]. The method of claim 4 [11] wherein said additional data is related to the payload of a watermark encoded in the body data.*

These claims are rejected by reference to the rejection of claim 1. For the reasons just-noted concerning claim 1, the Office has similarly failed to establish *prima facie* obviousness of claims 10 and 18.

14. Claim 25 (§103 Roese + Levy '899)

Claim 25 reads as follows:

> *25. A method of deterring unauthorized redistribution of video entertainment from a consumer's home network, the consumer's home network employing at least a computing device and a networking device;*
>
> *wherein acts performed by the computing device include:*
>
> *ascertaining restriction information for the video entertainment, said ascertaining including at least one of: (a) extracting restriction information from header data conveyed with the video entertainment; (b) obtaining restriction information from a remote repository associated with the video entertainment; or (c) discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment;*
>
> *dividing the video entertainment among payload portions of plural IP packets;*
>
> *including data indicating said ascertained restriction information in header portions of each of said IP packets; and*
>
> *sending the packets to the networking device;*
>
> *and wherein acts performed by the networking device comprise examining said included data and refusing to transmit the packets through the networking device to a different network if the included data indicates that the video entertainment should not be redistributed from the consumer's home network.*

The Final Action contends (middle of page 12) that Roese teaches all of claim 25 except:

extracting restriction information from header data conveyed with the video entertainment;

discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment; and *including data indicating said ascertained restriction information in header portions of each of said IP packets.*

(The three shortcomings of Roese cited by the Office and quoted above are not each necessary to claim 25; the claimed "ascertaining…" limitation is expressed as three alternatives – only one of which is required. Two are included in the quoted language.)

However, in addition to the shortcomings noted by the Office, Roese also does not disclose a computing device in a consumer's home network that divides video entertainment among payload portions of plural IP packets. Instead, in Roese, the dividing of content into packet form is understood to be done by a remote party. No device at a consumer's home performs this act.

Similarly, Roese does not teach a home networking device that refuses to transmit packets "to a different network if the included data indicates that the video entertainment should not be redistributed from the consumer's home network." No device at a consumer's home performs this act.

Thus the art – even if combined in the manner proposed – would still not yield the claimed arrangement. *Prima facie* obviousness has not been established.

Moreover, the Final Rejection contends (page 13, lines 3-4) that a packet header, per Levy '899, includes information pertaining to a watermark payload in each packet.

Again, this blurs the two arrangements in paragraph [0035] of Levy. But regardless – if the information is in the packet header as stated in the rejection (and claim), then it is not hidden. This nullifies the reason offered for using watermark data: providing restriction information "hidden from a user" (Final Rejection page 13, last line of first full paragraph).

Again, the Office has not met its burden of establishing obviousness. The rejection of claim 25 should be reversed.

15. Claim 26 (§103 Roese + Levy '899)

Claim 26 is allowable for its dependence from claim 25, and is also independently patentable. The claim reads as follows:

> *26. The method of claim 25 wherein the ascertaining includes extracting restriction information from header data conveyed with the video entertainment.*

(This limitation is the first of the three alternative limitations in the "ascertaining…" clause of claim 25.)

The Office cites Levy '899 for extracting restriction information from packet header data. But claim 25 poses this act as one done by the consumer's computing device *before* the packets are sent to the consumer's home networking device. That is, the "ascertaining…" of restriction information must *precede* "including…" data related to the restriction in header portions of each of the IP packets, as claimed.

An artisan following Levy's teachings would not reach such an arrangement.

Again, the Final Rejection has failed to establish *prima facie* obviousness.

16. Claim 28 (§103 Roese + Levy '899)

Claim 28 is allowable for its dependence from claim 25, and is also independently patentable. The claim reads as follows:

> *28. The method of claim 25 wherein the ascertaining includes discerning the restriction information by reference to data decoded from digital watermark information*

hidden within the video entertainment.

(This limitation is the third of the three alternative limitations in the "ascertaining…" clause of claim 25.)

Again, the Office cites Levy '899 for extracting restriction information by reference to digital watermark information hidden within the video content. But claim 25 poses this act as one done by the consumer's computing device *before* the packets are sent to the consumer's home networking device. That is, the "ascertaining…" of restriction information must *precede* "including…" data related to the restriction in header portions of each of the IP packets, as claimed.

Again, an artisan following Levy's teachings would not reach such an arrangement.

Again, the Final Rejection has failed to establish *prima facie* obviousness.

17. <u>Claim 27 (§103 Roese + Levy '899 + Levy '844)</u>

Claim 27 is allowable for its dependence from claim 25, and is also independently patentable. The claim reads as follows:

> *27. The method of claim 25 wherein the ascertaining includes obtaining restriction information from a remote repository associated with the video entertainment.*

(This limitation is the second of the three alternative limitations in the "ascertaining…" clause of claim 25.)

Levy '844 is also by the present Appellant.

Again, however, the claim requires that the restriction information is included in header portions of the IP packets. As such, it is not hidden. Since it is not hidden, the Final Rejection provides no indication why an artisan would have turned to Levy '899 for watermark teachings.

Again, the Final Rejection has failed to establish *prima facie* obviousness.

18. Claims 29-31 (§103 Roese + Levy '899 + Medvinsky)

The rejection of claims 29-31 stand or falls with the rejections of claims 1, 4 and 11, from which such claims depend.

VIII. CONCLUSION

The Board is requested to reverse the Final Rejections so that the application can be passed to issuance.

Date: October 21, 2009

CUSTOMER NUMBER 23735

Phone: 503-469-4800
FAX 503-469-4777

Respectfully submitted,

DIGIMARC CORPORATION

By /William Y. Conwell/
William Y. Conwell
Registration No. 31,943

IX. CLAIMS APPENDIX

1. A method of enforcing geographical restrictions on content redistribution in a TCP/IP network in which content is distributed in packet form, each packet including header data and content data, the header data comprising information about the packet and its payload, the method comprising the acts:

defining a geographical boundary across which certain content data does not pass, wherein said boundary is defined – at least in part – by a hardware firewall device; and

determining whether an IP packet should be regarded as conveying content that should not cross said boundary, by reference to one or more single-bit flags included in the header data of said packet;

wherein said one or more flag bits are related to the payload of a watermark in the content data.

2-3. (Canceled)

4. A method of providing entertainment content from a distributor to a home, while governing potential redistribution of the content from the home, the method including forming an IP packet having header data and body data, wherein the body data includes content data, and the header data includes a first destination address within the home to which the distributor intends the content data be delivered, the method comprising:

the distributor forming said header data to additionally include additional data specifying whether it is permissible to send a copy of the content data in the packet to a second destination address different than the first destination address, wherein the additional data has at least two states, respectively indicating:

(a) it is not permissible to send a copy of the content data in the packet to any second destination address; or

(b) it is not permissible to send a copy of the content data in the packet to any second destination address except to a second destination address within a domain that also includes the first destination address; and

wherein said domain comprises networked devices associated with a single family, and restriction on potential redistribution of the content is defined by reference to the intended first address.

5-6. (Canceled)

7. The method of claim 4 wherein a device associated with the first destination address has a first physical location and a device associated with the second destination address has a second physical location, and the additional data includes a field signaling that copying of data in said packet to said second destination address should be:

(a) permitted if the second physical location is physically proximate to the first physical location; and

(b) prohibited if the second physical location is physically remote from the first physical location.

8. The method of claim 7 wherein the first and second destination addresses are within a common domain.

9. The method of claim 7 wherein the first and second destination addresses both correspond to network devices associated with a single family.

10. The method of claim 4 wherein said additional data is related to the payload of a watermark encoded in the body data.

11. A method of data processing that includes receiving an IP packet having header data and body data, wherein the header data includes a first destination address, the first destination address corresponding to a device at a first physical location where delivery of the packet was intended by an originator thereof, the body data comprising content data, the method comprising – at said first physical location - interpreting additional data in the header of said packet as specifying whether it is permissible to re-transmit a copy of data in the packet - after receipt thereof at the first destination address - to a second destination address, wherein:

(a) if the additional data has a first state, prohibiting re-transmission of a copy of the content data in the packet to any second destination address; and

(b) if the additional data has a second state, prohibiting re-transmission of a copy of data in the packet to any second destination address other than a second destination address within a domain that also includes the first destination address.

12. (Canceled)

13. The method of claim 11, wherein said domain comprises networked devices associated with a single family.

14. The method of claim 11 wherein a device associated with the second destination address has a second physical location and wherein:

(a) if the second physical location is physically proximate to the first physical location, permitting copying of data in said packet to the second destination address; and

(b) if the second physical location is physically remote from the first physical location, prohibiting copying of data in said packet to the second destination address.

15. The method of claim 14 wherein the first and second destination addresses are within a common domain.

16. The method of claim 14 wherein the first and second destination addresses both correspond to network devices associated with a single family.

17. The method of claim 14 wherein the method includes determining whether the second physical location is physically remote from the first physically location by reference to whether the second destination address is served by a common firewall with the first destination address.

18. The method of claim 11 wherein said additional data is related to the payload of a watermark encoded in the body data.

19-24. (Canceled)

25. A method of deterring unauthorized redistribution of video entertainment from a consumer's home network, the consumer's home network employing at least a computing device and a networking device;

wherein acts performed by the computing device include:

ascertaining restriction information for the video entertainment, said ascertaining including at least one of: (a) extracting restriction information from header data conveyed with the video entertainment; (b) obtaining restriction information from a remote repository associated with the video entertainment; or (c) discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment;

dividing the video entertainment among payload portions of plural IP packets;

including data indicating said ascertained restriction information in header portions of each of said IP packets; and

sending the packets to the networking device;

and wherein acts performed by the networking device comprise examining said included data and refusing to transmit the packets through the networking device to a different network if the included data indicates that the video entertainment should not be redistributed from the consumer's home network.

26. The method of claim 25 wherein the ascertaining includes extracting restriction information from header data conveyed with the video entertainment.

27. The method of claim 25 wherein the ascertaining includes obtaining restriction information from a remote repository associated with the video entertainment.

28. The method of claim 25 wherein the ascertaining includes discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment.

29. The method of claim 1 wherein the determining comprises determining by reference to one single-bit flag.

30. The method of claim 4 wherein the additional data comprises a single bit flag, indicating either the first or second state.

31. The method of claim 11 wherein the additional data comprises a single bit flag, indicating either the first or second state.

X. EVIDENCE APPENDIX

None

XI. RELATED PROCEEDINGS APPENDIX

None